(12) UK Patent Application (19) GB (11) 2 385 343 (13) A

(43) Date of A Publication 20.08.2003

(21) Application No 0302937.8

(22) Date of Filing 10.02.2003

(30) Priority Data
(31) 10076993 (32) 15.02.2002 (33) US

(51) INT CL[7]
E21B 43/11 // E21B 43/1185

(52) UK CL (Edition V)
E1F FLT

(56) Documents Cited
None

(58) Field of Search
UK CL (Edition V) E1F
INT CL[7] E21B
Other: Online: EPODOC, WPI & JAPIO

(71) Applicant(s)
Schlumberger Holdings Limited
(Incorporated in the British Virgin Islands)
PO Box 71, Craigmuir Chambers,
Road Town, Tortola, British Virgin Islands

(72) Inventor(s)
Nolan C Lerche
James E Brooks
Simon L Farrent
Edward H Rogers

(74) Agent and/or Address for Service
Sensa
Gamma House, Enterprise Road,
Chilworth Science Park, SOUTHAMPTON,
Hampshire, SO16 7NS, United Kingdom

(54) Abstract Title
Interactive and secure activation of a tool

(57) Activation of a tool is governed by the receipt of an authorisation code and also data relating to the environment of the tool. If the environment data indicate that activation would be undesirable or unsafe, then the activation command fails. The arrangement is preferably used with a downhole perforating gun 104 or other explosive tool and the gathered information may include the depth and orientation of the gun, the density, composition, viscosity and bubble point of the surrounding fluid and the pressure and temperature. The authorisation signal may be encrypted and access to the surface control unit 100 may be restricted by password, swipe card or biometric requirements. Also disclosed are an explosive tool with a safety sub 106 having a switch to isolate the electrical arming circuits, and an explosives gun having a sensor with a communication line.

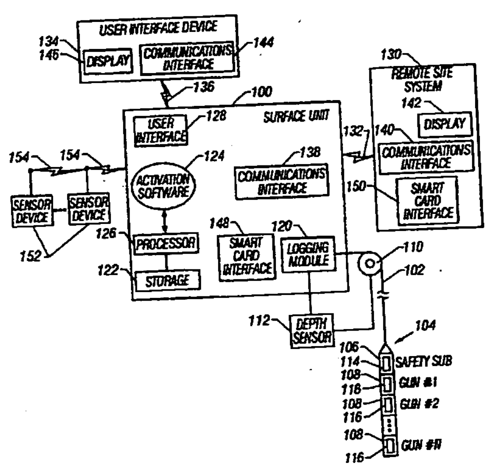

FIG. 1

At least one drawing originally filed was informal and the print reproduced here is taken from a later filed formal copy.

This print takes account of replacement documents submitted after the date of filing to enable the application to comply with the formal requirements of the Patents Rules 1995

GB 2 385 343 A

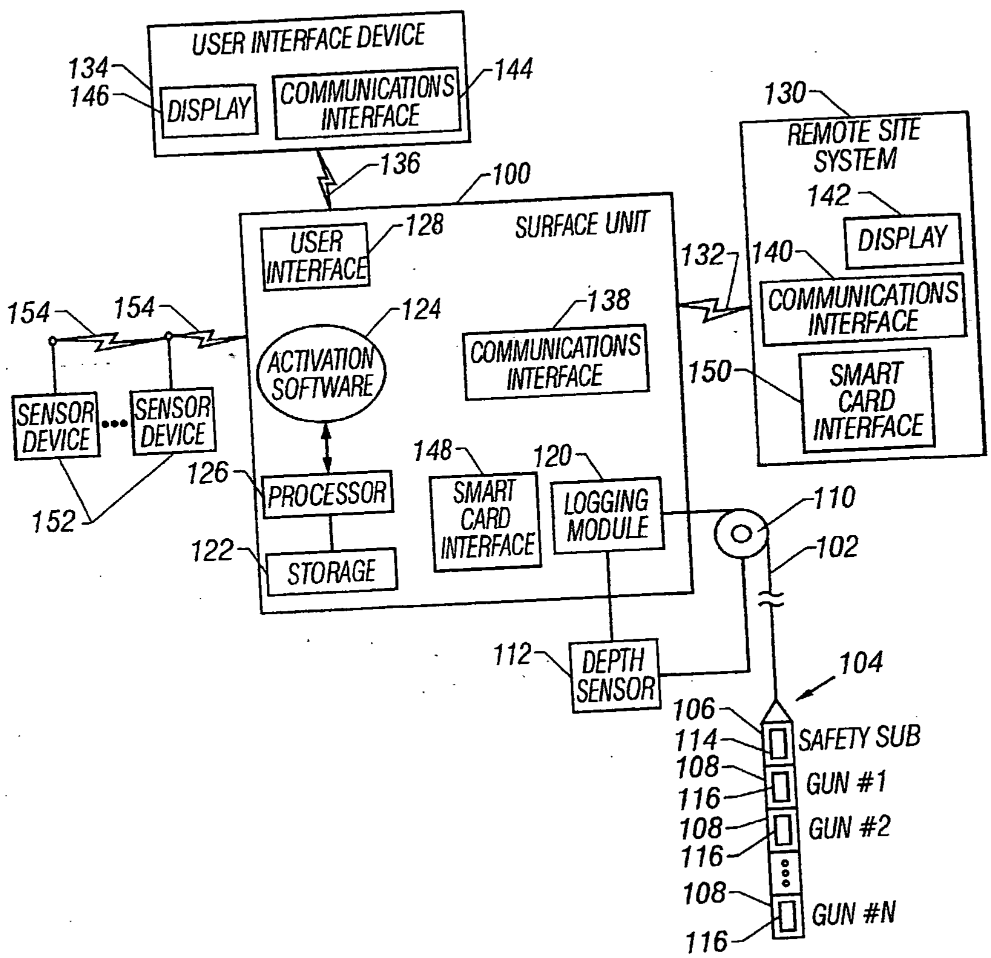
USER INTERFACE DEVICE
134
146
DISPLAY
COMMUNICATIONS INTERFACE
144
136
100
130
REMOTE SITE SYSTEM
142
DISPLAY
USER INTERFACE
128
SURFACE UNIT
132
140
COMMUNICATIONS INTERFACE
154
154
124
138
ACTIVATION SOFTWARE
COMMUNICATIONS INTERFACE
150
SMART CARD INTERFACE
SENSOR DEVICE
SENSOR DEVICE
148
120
126
PROCESSOR
SMART CARD INTERFACE
LOGGING MODULE
110
152
122
STORAGE
102
112
DEPTH SENSOR
104
106
SAFETY SUB
114
108
GUN #1
116
108
GUN #2
116
108
GUN #N
116

FIG. 1

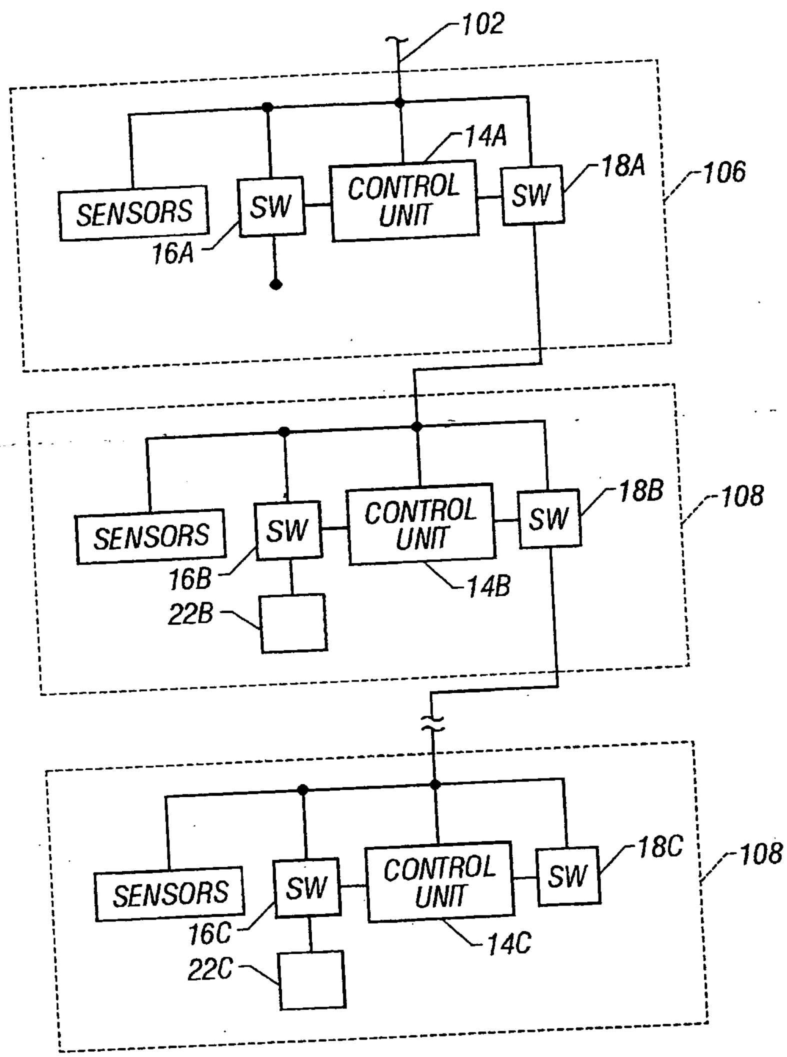
102
14A
18A
106
SENSORS
SW
CONTROL UNIT
SW
16A
18B
108
SENSORS
SW
CONTROL UNIT
SW
16B
14B
22B
18C
108
SENSORS
SW
CONTROL UNIT
SW
16C
14C
22C

FIG. 2

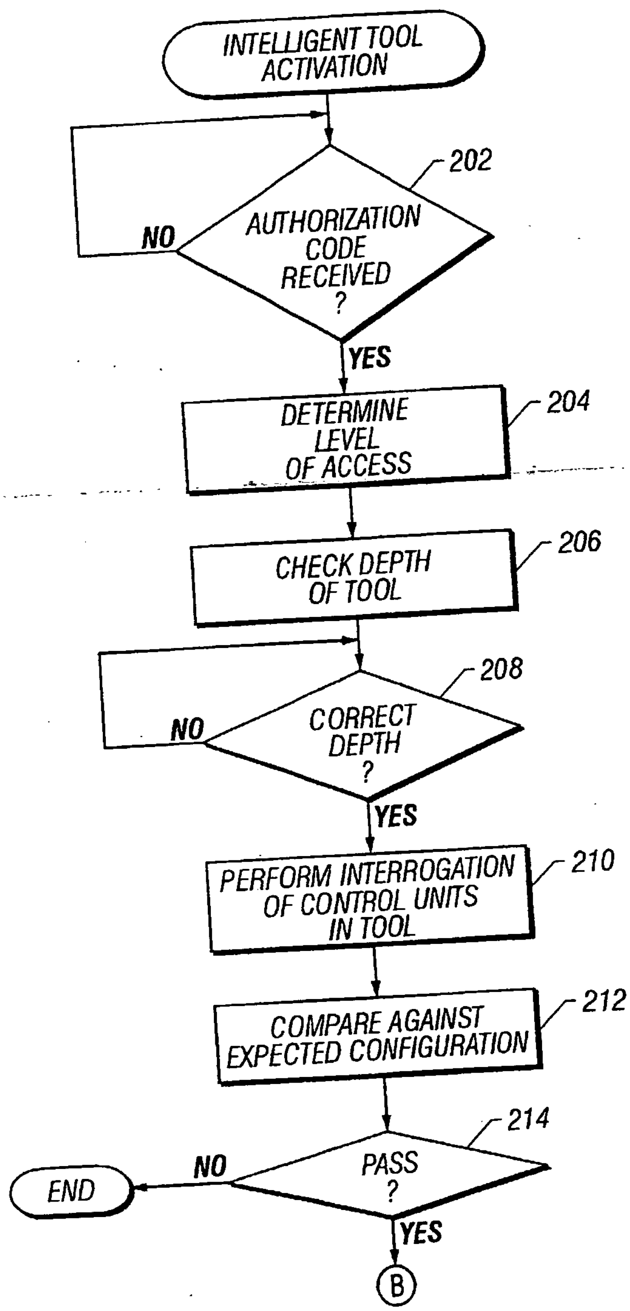
INTELLIGENT TOOL ACTIVATION
AUTHORIZATION CODE RECEIVED ?
202
NO
YES
DETERMINE LEVEL OF ACCESS
204
CHECK DEPTH OF TOOL
206
CORRECT DEPTH ?
208
NO
YES
PERFORM INTERROGATION OF CONTROL UNITS IN TOOL
210
COMPARE AGAINST EXPECTED CONFIGURATION
212
PASS ?
214
NO
END
YES
B

FIG. 3A

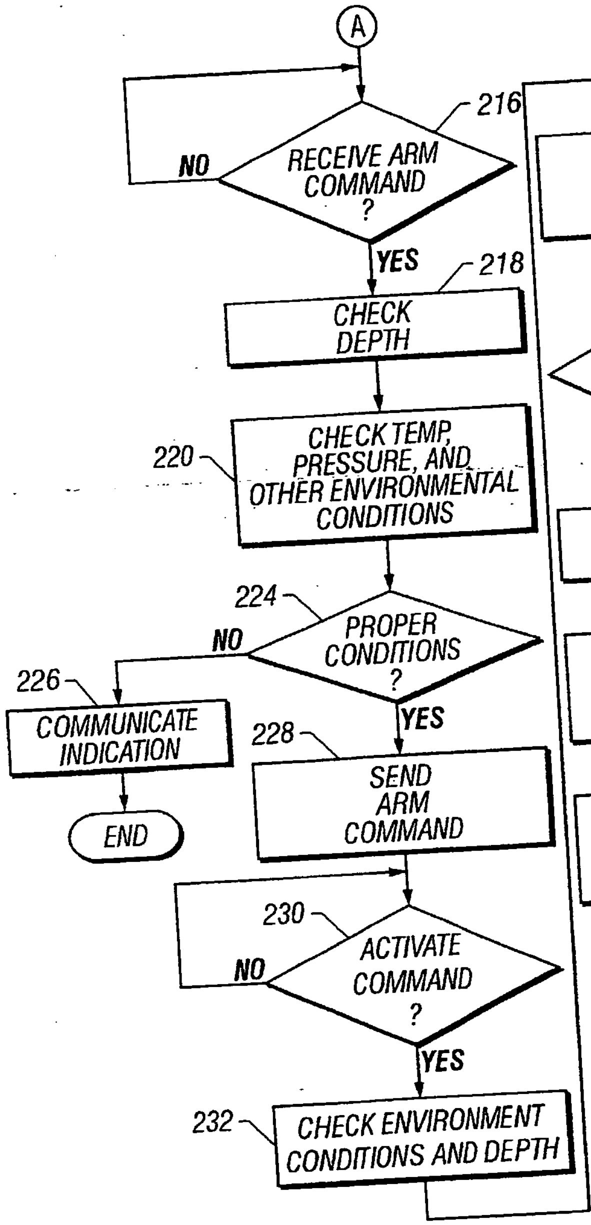
A
RECEIVE ARM COMMAND ?
216
NO
YES
CHECK DEPTH
218
CHECK TEMP, PRESSURE, AND OTHER ENVIRONMENTAL CONDITIONS
220
PROPER CONDITIONS ?
224
NO
YES
COMMUNICATE INDICATION
226
END
SEND ARM COMMAND
228
ACTIVATE COMMAND ?
230
NO
YES
CHECK ENVIRONMENT CONDITIONS AND DEPTH
232
CHECK GUN POSITION AND ORIENTATION
234
PROPER CONDITION AND POSITION ?
236
NO
END
YES
SEND ACTIVATE COMMAND
238
COLLECT DATA FROM SENSORS AFTER ACTIVATION
240
COMMUNICATE COLLECTED DATA
242

FIG. 3B

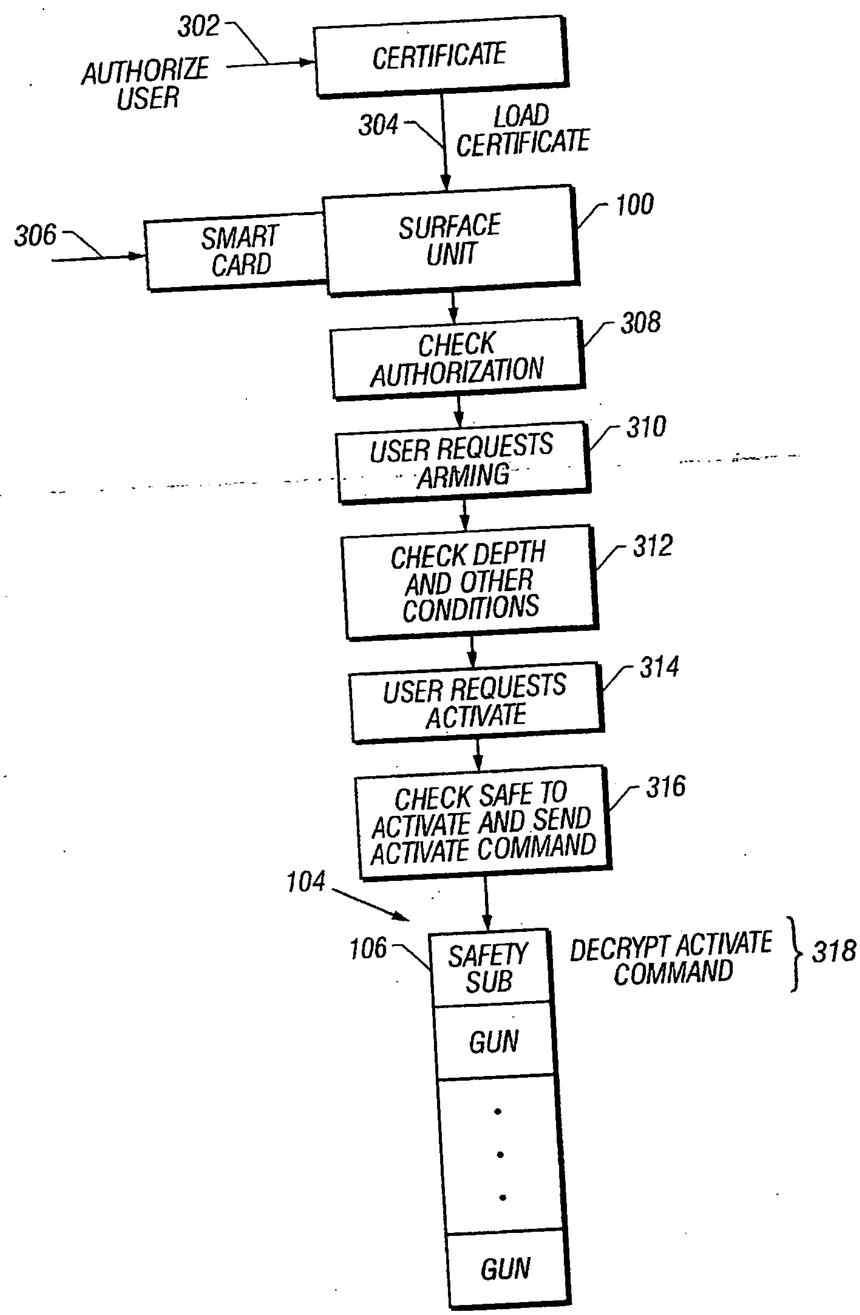
302
AUTHORIZE USER
CERTIFICATE
304
LOAD CERTIFICATE
306
SMART CARD
SURFACE UNIT
100
CHECK AUTHORIZATION
308
USER REQUESTS ARMING
310
CHECK DEPTH AND OTHER CONDITIONS
312
USER REQUESTS ACTIVATE
314
CHECK SAFE TO ACTIVATE AND SEND ACTIVATE COMMAND
316
104
106
SAFETY SUB
DECRYPT ACTIVATE COMMAND
318
GUN
GUN

FIG. 4

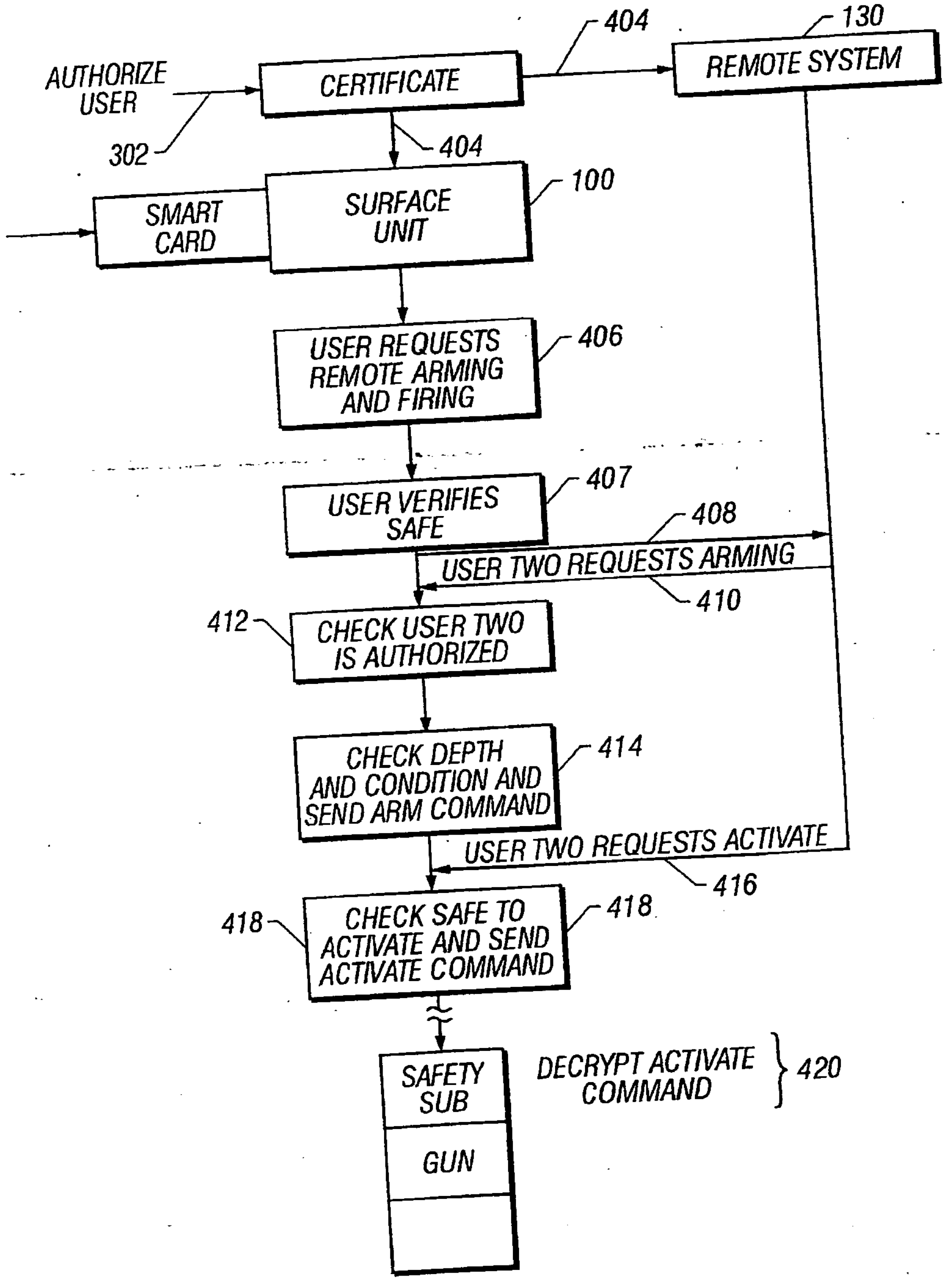
AUTHORIZE USER
302
CERTIFICATE
404
REMOTE SYSTEM
130
404
SMART CARD
SURFACE UNIT
100
USER REQUESTS REMOTE ARMING AND FIRING
406
USER VERIFIES SAFE
407
408
USER TWO REQUESTS ARMING
410
412
CHECK USER TWO IS AUTHORIZED
CHECK DEPTH AND CONDITION AND SEND ARM COMMAND
414
USER TWO REQUESTS ACTIVATE
416
418
CHECK SAFE TO ACTIVATE AND SEND ACTIVATE COMMAND
418
SAFETY SUB
GUN
DECRYPT ACTIVATE COMMAND
420

FIG. 5

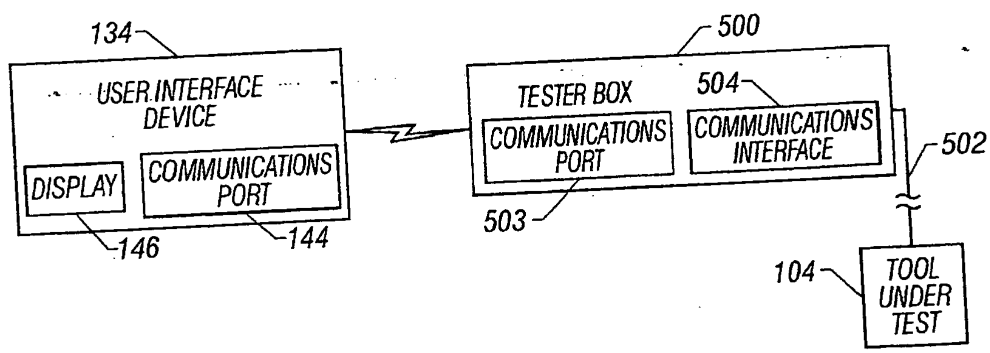
134
USER INTERFACE DEVICE
DISPLAY
COMMUNICATIONS PORT
146
144
500
TESTER BOX
504
COMMUNICATIONS PORT
COMMUNICATIONS INTERFACE
503
502
104
TOOL UNDER TEST

FIG. 6

2385343

INTERACTIVE AND/OR SECURE ACTIVATION OF A TOOL

CROSS REFERENCE TO RELATED APPLICATIONS

[001] This is a continuation-in-part of U.S. Serial No. 09/997,021, filed November 28, 2001, which is a continuation-in-part of U.S. Serial No. 09/179,507, filed October 27, 1998.

TECHNICAL FIELD

[002] The invention relates generally to interactive and/or secure activation of tools, such as tools used in well, mining, and seismic applications.

BACKGROUND

[003] Many different types of operations can be performed in a wellbore. Examples of such operations include firing guns to create perforations, setting packers, opening and closing valves, collecting measurements made by sensors, and so forth. In a typical well operation, a tool is run into a wellbore to a desired depth, with the tool being activated thereafter by some mechanism, e.g., hydraulic pressure activation, electrical activation, mechanical activation, and so forth.

[004] In some cases, activation of downhole tools creates safety concerns. This is especially true for tools that include explosive devices, such as perforating tools. To avoid accidental detonation of explosive devices in such tools, the tools are typically transferred to the well site in an unarmed condition, with the arming performed at the well site. Also, there are safety precautions taken at the well site to ensure that the explosive devices are not detonated prematurely. Another safety concern that exists at a well site is the use of wireless, especially radio frequency (RF), devices, which may inadvertently activate certain types of explosive devices. As a result, such wireless devices are usually not allowed at a well site, thereby limiting communications options that are available to well operators. Yet another

concern associated with using explosive devices at a well site is the presence of stray voltages that may inadvertently detonate the explosive devices.

[005] A further safety concern with explosive tools is that they may fall into the wrong hands. Such explosive tools pose great danger to persons who do not know how to handle explosive tools, or who want to use the explosive tools to harm others.

[006] In addition to well applications, other applications that involve the use of explosive tools include mining applications and seismic applications. Similar types of safety concerns exist with such other types of explosive tools. Thus, a need continues exist to enhance the safety associated with the use of explosive tools as well as with other types of tools. Also, a need continues to exist to enhance the flexibility of controlling the operation of such explosive tools.

SUMMARY OF THE INVENTION

[007] In general, an improved method and apparatus is provided to enhance the safety and flexibility associated with use of a tool. For example, a method of activating a tool includes checking an authorization code of a user to verify that the user has access to activate the tool. In addition, data pertaining to an environment around the tool is received. Activation of the tool is enabled in response to the authorization code and the data indicating that the environment around the tool meets predetermined one or more criteria for activation of the tool.

[008] Other or alternative features will become apparent from the following description, the drawings, and the claims.

BRIEF DESCRIPTION OF THE DRAWINGS

[009] Fig. 1 is block diagram of an example arrangement of control systems, sensors, and a downhole well tool.

[0010] Fig. 2 is a block diagram of a perforating tool, according to one embodiment, that can be used in the system of Fig. 1.

[0011] Figs. 3A-3B are a flow diagram of a process performed by a surface unit in accordance with an embodiment.

[0012] Figs 4 and 5 illustrate processes for secure and interactive activation of a perforating tool.

[0013] Fig. 6 is a block diagram of an example test arrangement including a tester box coupled to a tool under test, and a user interface device to control the tester box.

DETAILED DESCRIPTION OF THE INVENTION

[0014] In the following description, numerous details are set forth to provide an understanding of the present invention. However, it will be understood by those skilled in the art that the present invention may be practiced without these details and that numerous variations or modifications from the described embodiments may be possible.

[0015] As used here, the terms "up" and "down"; "upper" and "lower"; "upwardly" and downwardly"; "upstream" and "downstream"; "above" and "below"; and other like terms indicating relative positions above or below a given point or element are used in this description to more clearly describe some embodiments of the invention. However, when applied to equipment and methods for use in wells that are deviated or horizontal, such terms may refer to a left to right, right to left, or other relationship as appropriate.

[0016] Referring to Fig. 1, a system according to one embodiment includes a surface unit 100 that is coupled by cable 102 (e.g., a wireline) to a tool 104. In the example shown in Fig. 1, the tool 104 is a tool for use in a well. For example, the tool 104 can include a perforating tool or other tool containing explosive devices, such as pipe cutters and the like. In other embodiments, other types of tools can be used for performing other types of operations in a well. For example, such

other types of tools include tools for setting packers, opening or closing valves, logging, taking measurements, core sampling, and so forth. In the embodiments described below, safety issues associated with well tools containing explosive devices are discussed. However, similar methods and apparatus can be applied to tools having explosive devices in other applications, e.g., mining, seismic acquisition, surface demolition, armaments, and so forth.

[0017] The tool 104 includes a safety sub 106 and a plurality of guns 108. In one embodiment, the safety sub 106 differs from the gun 108 in that the safety sub 106 does not include explosive devices that are present in the guns 108. The safety sub 106 serves one of several purposes, including providing a quick connection of the tool 104 to the cable 102. Additionally, the safety sub 106 allows electronic arming of the perforating tool 104 downhole instead of at the surface. Because the safety sub 106 does not include explosive devices, it provides electrical isolation between the cable 102 and the guns 108 so that electrical activation of the guns 108 is disabled until the safety sub 106 has been activated to close an electrical connection.

[0018] In the example of Figure 1, the cable 102 is run through a winch assembly 110, which is coupled to a depth sensor 112. The depth sensor 112 monitors the rotation of the winch assembly 110 to determine the depth of the perforating tool 104. The data relating to the depth of the tool 104 is communicated to the surface unit 100.

[0019] In some systems, an internal (hardware or software) drive system can be used to simulate that the tool 104 has descended to a certain depth in the wellbore, even though the tool 104 is still at the earth surface. The depth sensor 112 can be used by the surface unit to verify that the tool 104 has indeed been lowered into the wellbore to a target depth. As a safety precaution, the ability to use the output of the internal hardware or drive system to enable activation of the tool 104 is prohibited.

[0020] The perforating tool 104 also includes a number of sensors, such as sensors 114 in the safety sub and sensors 116 in the guns 108. Although Fig. 1 shows each gun 108 as containing sensors 116, less than all of the guns can be selected to include sensors in other embodiments.

[0021] Data from the sensors 114 and 116 are communicated over the cable 102 to a logging module 120 in the surface unit 100. The logging module 120 is capable of performing bi-directional communications with the sensors 114 and 116 over the cable 102. For example, the logging module 120 is able to issue commands to the sensors 114 and 116 to take measurements, and the logging module 120 is then able to receive measurement data from the sensors 114 and 116. Data collected by the logging module 120 is stored in a storage 122 in the surface unit 100. Examples of the storage 122 include magnetic media (e.g., a hard disk drive), optical media (e.g., a compact disk or digital versatile disk), semiconductor memories, and so forth. The surface unit 100 also includes activation software 124 that is executable on a processor 126. The activation software 124 is responsible for managing the activation of the perforating tool 104 in response to user commands. The user commands can be issued from a number of sources, such as directly through a user interface 128 at the surface unit 100, from a remote site system 130 over a communications link 132, or from a portable user interface device 134 over a communications link 136.

[0022] In one embodiment, the communications links 132 and 136 include wireless links, in the form of radio frequency (RF) links, infrared (IR) links, and the like. Alternatively, the communications links 132 and 136 are wired links. The surface unit 100 includes a communications interface 138 for communicating with the user interface device 134 and the remote site system 130 over the respective links. The remote site system 130 also includes a communications interface 140 for communicating over the communications link 132 to the surface unit 100. Also, the remote site system 130 includes a display 142 for presenting

information (e.g., status information, logging information, etc.) associated with the surface unit 100.

[0023] The user interface device 134 also includes a communications interface 144 for communicating over the communications link 136 with the surface unit 100. Additionally, the user interface device 134 includes a display 146 to enable the user to view information associated with the surface unit 100. An example of the user interface device 134 is a personal digital assistant (PDA), such as a PALM® device, a WINDOWS® CE device, or other like device. Alternatively, the user interface device 134 includes a laptop or notebook computer.

[0024] In accordance with an embodiment, a security feature of the surface unit 100 is a smart card interface 148 for interacting with a smart card of a user. The smart card interface 148 is capable of reading identification information of the user (e.g., a digital signature, a user code, an employee number, and so forth). The activation software 124 uses this identification information to determine if the user is authorized to access the surface unit 100 and to perform activation of the perforating tool 104. The identification information is part of the "authorization code" provided by a user to gain access to the surface unit 100.

[0025] A smart card is basically a card with an embedded processor and storage, with the storage containing various types of information associated with a user. Such information includes a digital signature, a user profile, and so forth.

[0026] In an alternative embodiment, instead of a smart card interface 148, the surface unit 100 can include another type of security feature, such as providing a prompt in which a user has to enter his or her user name and password. In yet another embodiment, the security mechanism of the surface unit 100 includes a biometric device to scan a biometric feature (e.g., fingerprint) of the user. The user interface device 134 can similarly include a smart card reader or biometric input device.

[0027] Alternatively, the user enters information and commands using either the user interface device 134 or the remote site system 130. The user interface device 134 may itself store an authorization code, such as in the form of a user code, digital signature, and the like, that is communicated to the surface unit 100 with any commands issued by the user interface device 134. Only authorized user interface devices 134 are able to issue commands that are acted on by the surface unit 100. Although not shown, the user interface device 134 can optionally include a smart card interface to interact with the smart card of the user.

[0028] In the example shown, the remote site system 130 also includes a smart card interface 150. Thus, before a user is able to issue commands from the remote site system 130 to the surface unit 100 to perform various actions, the user must be in possession of a smart card that enables access to the various features provided by the surface unit 100.

[0029] In this way, the surface unit 100 cannot be accessed by unauthorized users. Therefore, safety problems associated with the unauthorized use of the perforating tool 104 is avoided.

[0030] Another safety feature offered by the perforating tool 104 is that each of the guns 108 is associated with a unique code or identifier. This code or identifier must be issued by the surface unit 100 with an activate command for the gun 108 to be activated. If the code or identifier is not provided, then the gun 108 cannot be fired. Thus, if the perforating tool 104 is stolen or is lost, unauthorized users will not be able to activate the guns 108 since they do not know what the codes or identifiers are. The safety sub 106 is also associated with a unique code or identifier that must be received by the safety sub 106 for the safety sub 106 to be activated to electrically arm the perforating tool 104.

[0031] Another feature allowed by using unique codes or identifiers for the guns 108 is that the guns can be traced (to enable the tracking of lost or misplaced

guns). Also, the unique codes or identifiers enable inventory control, allowing a well operator to know the equipment available for well operations.

[0032] Yet another safety feature associated with the guns 108 according to one embodiment is that they use exploding foil initiators (EFIs), which are safe in an environment in which wireless signals, such as RF signals, are present. As a result, this feature of the guns 108 enables the use of RF communications between the surface unit 100 and the remote site system 130 and with the user interface device 134. However, in other embodiments, conventional detonators can be used in the perforating tool 104, with precautions taken to avoid use of RF signals. The EFI detonator is one example of an electro-explosive device (EED) detonator, with other examples including an exploding bridge wire (EBW) detonator, semiconductor bridge detonator, hot-wire detonator, and so forth.

[0033] Another feature offered by the surface unit 100 according to some embodiments is the ability to perform "interactive" activation of the perforating tool 104. The "interactive" activation feature refers to the ability to communicate with the sensors 114 and/or 116 in the perforating tool 104 before, during, and after activation of the perforating tool 104. For example, the sensors 114 and/or 116 are able to take pressure measurements (to determine if an under balance or over balance condition exists prior to perforating), take temperature measurements (to verify explosive temperature ratings are not exceeded), and take fluid density measurements (to differentiate between liquid and gas in the wellbore). Also, the surface unit 100 is able to interact with the depth sensor 112 to determine the depth of the perforating tool 104. This is to ensure that the perforating tool 104 is not activated prior to it being at a safe depth in the wellbore. As an added safety precaution, a user will be prevented from artificially setting the depth of the perforating tool below a predetermined depth for test purposes. In some systems, such a depth can be set by software or hardware to simulate the tool being in the

wellbore. However, due to safety concerns, artificially setting the depth to a value where a gun is allowed to be activated is prohibited.

[0034] The sensors 114 and/or 116 may also include voltage meters to measure the voltage of the cable 102 at the upper head of the perforating tool 104, the voltages at the detonating devices in the respective guns 108, the amount of current present in the cable 102, the impedance of the cable 102 and other electrical characteristics. The sensors may also include accelerometers for detecting tool movement as well as shot indication. Shot indication can be determined from waveforms provided by accelerometers over the cable 102 to the surface unit 100. Alternatively, the waveform of the discharge voltage on the cable 102 can be monitored to determine if a shot has occurred.

[0035] The sensors 114 and/or 116 may also include moisture detectors to detect if excessive moisture exists in each of the guns 108. Excessive moisture can indicate that the gun may be flooded and thus may not fire properly or at all.

[0036] The sensors may also include a position or orientation sensor to detect the position or orientation of a gun in well, to provide an indication of well deviation, and to detect correct positioning (e.g., low side of casing) before firing the gun. Also, the sensors may include a strain-gauge bridge sensor to detect external strain on the perforating tool 104 that may be due to pulling or other type of strain on the housing or cable head of a gun that is stuck in the well. Other types of sensors include acoustic sensors (e.g., a microphone), and other types of pressure gauges.

[0037] Other types of example sensors include equipment sensors (e.g., vibration sensors), sand detection sensors, water detection sensors, scale detectors, viscosity sensors, density sensors, bubble point sensors, composition sensors, infrared sensors, gamma ray detectors, H_2S detectors, CO_2 detectors, casing collar locators, and so forth.

[0038] One of the aspects of the sensors 116 is that they are destroyed with firing of the guns 108. However, the sensors 114 in the safety sub 106 may be able to survive detonation of the guns 108. Thus, these sensors 114 can be used to monitor well conditions (e.g., measure pressure, temperature, and so forth) before, during, and after a perforating operation.

[0039] In addition to the sensors that are present in the perforating tool 104, other sensors 152 can also be located at the earth surface. The sensors 152 are able to detect shock or vibrations created in the earth due to activation of the perforating tool 104. For example, the sensors 152 may include geophones. The sensors 152 are coupled by a communications link 154, which may be a wireless link or a wired link, to the surface unit 100. Data from the sensors 152 to the surface unit 100 provide an indication of whether the perforating tool 104 has been activated.

[0040] The safety sub 106 and guns 108 of the perforating tool 104 are shown in greater detail in Fig. 2. In the example shown in Fig. 2, the safety sub 106 includes a control unit 14A, and the guns 108 include control units 14B, 14C. Although only two guns 108 are shown in the example Fig. 2, other embodiments may include additional guns 108. Each control unit 14 is coupled to switches 16 and 18 (illustrated at 16A-16C and 18A-18C). The switches 18A-18C are cable switches that are controllable by the control units 14A-14C, respectively, between on and off positions to enable or disable current flow through portions of the cable 102. When the switch 18 is off, then the portion of the cable 102 below the switch 18 is isolated from the portion of the cable 102 above the switch 18. The switches 16A-16C are detonating switches.

[0041] In the safety sub 106, the detonating switch 16A is not connected to a detonating device. However, in the guns 108, the detonating switches 16B, 16C are connected to detonating devices 22B, 22C, respectively. If activated to an on position, a detonating switch 16 allows electrical current to flow to a coupled detonating device 22 to activate the detonating device. The detonating device

22B, 22C includes an EFI detonator or other detonators. The detonating devices 22B, 22C are ballistically coupled to explosives, such as shaped charges or other explosives, to perform perforating.

[0042] As noted above, the safety sub 106 provides a convenient mechanism for connecting the perforating tool 104 to the cable 102. This is because the safety sub 106 does not include a detonating device 22 or any other explosive, and thus does not pose a safety hazard. The switch 18A of the safety sub 106 is initially in the open position, so that all guns of the perforating tool 104 are electrically isolated from the cable 102 by the safety sub 106. Because of this feature, electrically arming of the perforating tool 104 does not occur until the perforating tool 104 is positioned downhole and the switch 18A is closed.

[0043] Another feature allowed by the safety sub 106 is that the guns 108 can be pre-armed (by connecting each detonating device 22 in the gun 108) during transport or other handling of the perforating tool 104. Thus, even though the perforating tool 104 is transported ballistically armed, the open switch 18A of the safety sub 106 electrically isolates the guns 108 from any activation signal during transport or other handling.

[0044] Figs. 3A-3B are a flow diagram of a tool activation process, which is performed by the activation software 124 according to one embodiment. Before access is provided for activating the perforating tool 104, the activation software 124 checks (at 202) if an authorization code has been received. The authorization code includes a digital signature, a user code, a user name and password, or some other code. The authorization code can be stored on a smart card and communicated to the surface unit 100 through the smart card interface 148. Alternatively, the authorization code can be manually entered by the user through a user interface.

[0045] If an authorization code has been received and verified, the activation software 124 determines (at 204) the level of access provided to the user. Users

are assigned a hierarchy of usage levels, with some users provided with a higher level of access while others are provided with a lower level of access. For example, a user with a higher level of access is authorized to activate the perforating tool to fire guns. A user with a lower access level may be able only to send inquiries to the perforating tool to determine the configuration of the perforating tool, and possibly, to perform a test of the perforating tool (without activating the detonating devices 22 in the perforating tool 104).

[0046] The activation software 24 also checks (at 206) for a depth of the perforating tool 104 in the well. Activation of the perforating tool 104 is prohibited unless the perforating tool 104 is at the correct depth. While the perforating tool 104 is not at a correct depth, as determined (at 208), further actions are prevented. However, once the perforating tool 104 is at the correct depth, the activation software 124 performs (at 210) various interrogations of control units 14 in the perforating tool 100. Interrogations may include determining the positions of switches 16 and 18 in the perforating tool 104, the status of the control unit 14, the configuration and arrangement of the perforating tool 104 (e.g., number of guns, expected identifications or codes of each control unit, etc.), and so forth.

[0047] Once the status information has been received from the perforating tool 104, the activation software 124 compares (at 212) the information against an expected configuration of the perforating tool 104. Based on the interrogations and the comparison performed at 210 and 212, the activation software 124 determines (at 214) if the perforating tool 104 is functioning properly or is in the proper configuration. If not, then the activation process ends with the tool 104 remaining deactivated. However, if the tool is determined to be functioning properly and in the expected configuration, the activation software 124 waits (at 216) for receipt of an arm command from the user. The arm command can be

provided by the user through the user interface 128 of the surface unit 100, through the user interface device 134, or through the remote site system 130.

[0048] Upon receipt of the arm command, the activation software 124 checks (at 218) the depth of the perforating tool 104 again. This is to ensure that the perforating tool 104 has not been raised from its initial depth.

[0049] Next, the activation software 124 checks (at 220) for various downhole environment conditions, including pressure, temperature, the presence of gas or liquid, the deviation of the wellbore, and so forth.

[0050] If the proper condition is not present, as determined at 224, the activation software 124 communicates (at 226) an indication to the user, such as through the user interface 128 of the surface unit 100, the display 146 of the user interface device 134, or the display 142 of the remote site system 130. Arming is prohibited.

[0051] However, if the condition of the well and the position of the perforating tool 104 is proper, the activation software 124 issues an arm command (at 228) to the perforating tool 100. The arm command is received by the safety sub 106, which closes the cable switch 18A in response to the arm command. Optionally, the cable switches 18B, 18C can also be actuated closed at this time.

[0052] The activation software 124 waits (at 230) for receipt of an activate command from the user. Upon receipt of the activate command, the activation software 124 re-checks (at 232) the environment conditions and the depth of the penetrating tool. The activation software 124 also checks (at 234) the gun position and orientation. It may be desirable to shoot the gun at a predetermined angle with respect to the vertical. Also, the shaped charges of the perforating tool 104 may be oriented to shoot in a particular direction, so the orientation has to be verified.

[0053] If the environment condition and gun position is proper, as determined at 236, the activation software 124 sends (at 238) the activate command to the

perforating tool 104. The activate command may be encrypted by the activation software 124 for communication over the cable 102. The control units 14 in the perforating tool 104 are able to decrypt the encrypted activate command. In one embodiment, the activate command is provided with the proper identifier code of each control unit 14. Each control unit 14 checks this code to ensure that the proper code has been issued before activating the appropriate switches 16 and 18 to fire the guns 108 in the perforating tool 104.

[0054] In one sequence, the guns 108 of the perforating tool 104 are fired sequentially by a series of activate commands. In another sequence, the activate command is provided simultaneously to all guns 108, with each gun 108 preprogrammed with a delay that specifies the delay time period between the receipt of the activate command and the firing of the gun 108. The delays in plural guns 108 may be different.

[0055] During and after activation of the perforating tool 104, measurement data is collected (at 240) from the various sensors 114, 116, and 152. The collected measurement data is then communicated (at 242) to the user.

[0056] Fig. 4 illustrates a flow diagram of a process of performing secure activation of an explosive tool, such as the perforating tool 104, according to one embodiment. A central management site (not shown) provides (at 302) a profile of a user that includes his or her associated identifier, authorization code, personal identification number (PIN) code, digital signature, and access level. This profile is loaded as a certificate (at 304) into the surface unit 100, where it is stored in the storage 122. During use, a user inserts (at 306) his or her smart card into the smart card interface 148 of the surface unit 100. The surface unit 100 may prompt for a PIN code through the user interface 128, which is then entered by the user. The surface unit 100 checks (at 308) to ensure that a user is authorized to use a system based on the stored certificate and notifies the user of access grant.

[0057] Next, the user requests (at 310) arming of the perforating tool 104, which is received by the surface unit 100. In response, as discussed above, the surface unit 100 checks (at 312) the depth of the perforating tool 104 and the data from other sensors from the perforating tool 104 to determine if the perforating tool 104 is safe to arm.

[0058] The user then issues a fire command (at 314), which is received by the surface unit 100. The surface unit 100 then checks (at 316) that the perforating tool 104 is safe to activate, and if so, sends an encrypted activate command to the perforating tool 104.

[0059] The control unit 14A in the safety sub 106 stores a private key at manufacture. This private key is used by the control unit 14A in the safety sub 106 to decrypt the activate command (at 318). The decrypted activate command is then forwarded to the guns 108 to fire the guns.

[0060] Fig. 5 illustrates a flow diagram of a process of remotely activating the perforating tool 104. In the context of Fig. 1, the remote activation is performed by a user at the remote site system 130. In the example of Fig. 5, two users are involved in remotely activating the perforating tool 104, with user 1 at the well site and user 2 at the remote site system 130. As before, a central management system authorizes user names and their associated information and access levels (at 302) and communicates certificates containing the profiles (at 404) to the surface unit 100 and to the remote site system 130 for storage.

[0061] At the surface unit 100, user 1 inserts (at 406) his or her smart card into the surface unit 100, along with the user's PIN code, to request remote arming and activation of the perforating tool 104. This indication is communicated (at 408) from the surface unit 100 to the remote site system 130 over the communications link 132. User 1 also verifies (at 407) that all is safe and ready to fire at the surface unit 100.

[0062] User 2 inserts his or her smart card into the smart card interface 150 of the remote site system 130 to gain access to the remote site system 130. Once authorized, user 2 requests (at 410) arming of the perforating tool 104. The surface unit 100 checks (at 412) that user 2 is authorized by accessing the certificate stored in the surface unit 100. This check can alternatively be performed by the remote site system 130.

[0063] The surface unit 100 then checks (at 414) the depth of the perforating tool 104 along with data from other sensors of the perforating tool 104 to ensure that the perforating tool 104 is safe to arm. Once the verification has been performed and communicated back to the remote site system 130, user 2 issues an activate command (at 416) at the remote site system 130. The surface unit 100 checks (at 418) to ensure that the perforating tool 104 is safe to activate, and then sends an encrypted activate command. The encrypted activate command is received by the safety sub 106, with the encrypted activate command decrypted (at 420) by the control unit 14A in the safety sub 106.

[0064] According to some embodiments of the invention, another feature is the ability to test the perforating tool 104 to ensure the perforating tool 104 is functioning properly. The test can be performed at the well site or at an assembly shop that is remote from the well site. To do so, as shown in Fig. 6, a tester box 500 is coupled to the perforating tool 104 over a communications link 502 through a communications interface 504. If the test is performed at the well site, the tester box 500 can be implemented in the surface unit 100. At the assembly shop or at some other location, the tester box 500 is a stand-alone unit. The tester box 500 includes a communications port 503 that is capable of performing wireless communications with communications port 144 in the user interface device 134. The communications can be in the form of IR communications, RF communications, or other forms of wireless communications. The

communications between the user interface device 134 and the tester box 500 can also be over a wired link.

[0065] In one embodiment, various graphical user interface (GUI) elements (e.g., windows, screens, icons, menus, etc.) are provided in the display 146 of the user interface device 134. The GUI elements include control elements such as menu items or icons that are selectable by a user to perform various acts. The GUI elements also include display boxes or fields in which information pertaining to the perforating tool 104 is displayed to the user.

[0066] In response to user selection of various GUI elements, the user interface device 134 sends commands to the tester box 500 to cause a certain task to be performed by control logic in the tester box 500. Among the actions taken by the tester box 500 is the transmission of signals over the cable 502 to test the components of the perforating tool 104. Feedback regarding the test is communicated back to the tester box 500, which in turn communicates data over the wireless medium to the user interface device 134, where the information is presented in the display 146. As an added safety feature, the tester box 500 can also include a smart card reader or biometric input device to verify user authorization.

[0067] A more detailed description of the tester box 500 and components in the perforating tool 104 to enable this testing feature is discussed in greater detail in U.S. Serial No. 09/997,021, entitled "Communicating with a Tool," filed November 28, 2001, which is hereby incorporated by reference.

[0068] The various systems and devices discussed herein each includes various software routines or modules. Such software routines or modules are executable on corresponding control units or processors. Each control unit or processor includes a microprocessor, a microcontroller, a processor card (including one or more microprocessors or microcontrollers), or other control or computing devices. As used here, a "controller" refers to a hardware component, software component,

or a combination of the two. Although used in the singular sense, a "controller" can also refer to plural hardware components, plural software components, or a combination thereof.

[0069] The storage devices referred to in this discussion include one or more machine-readable storage media for storing data and instructions. The storage media include different forms of memory including semiconductor memory devices such as dynamic or static random access memories (DRAMs or SRAMs), erasable and programmable read-only memories (EPROMs), electrically erasable and programmable read-only memories (EEPROMs) and flash memories; magnetic disks such as fixed, floppy and removable disks; other magnetic media including tape; and optical media such as compact disks (CDs) or digital video disks (DVDs). Instructions that make up the various software routines or modules in the various devices or systems are stored in respective storage devices. The instructions when executed by a respective control unit or processor cause the corresponding node or system to perform programmed acts.

[0070] The instructions of the software routines or modules are loaded or transported to each device or system in one of many different ways. For example, code segments including instructions stored on floppy disks, CD or DVD media, a hard disk, or transported through a network interface card, modem, or other interface device are loaded into the device or system and executed as corresponding software routines or modules. In the loading or transport process, data signals that are embodied in carrier waves (transmitted over telephone lines, network lines, wireless links, cables, and the like) communicate the code segments, including instructions, to the device or system. Such carrier waves are in the form of electrical, optical, acoustical, electromagnetic, or other types of signals.

[0071] While the invention has been disclosed with respect to a limited number of embodiments, those skilled in the art, having the benefit of this disclosure, will

appreciate numerous modifications and variations therefrom. It is intended that the appended claims cover such modifications and variations as fall within the true spirit and scope of the invention.

<u>CLAIMS</u>

What is claimed is:

1. A method of activating a tool, comprising:

checking an authorization code of a user to verify that the user has access to activate the tool;

receiving data pertaining to an environment around the tool; and

enabling activation of the tool in response to the authorization code and the data indicating that the environment around the tool meets predetermined one or more criteria for activation of the tool.

2. The method of claim 1, further comprising:

receiving a user command to activate the tool; and

sending an activate command to the tool if activation of the tool is enabled.

3. The method of claim 2, wherein sending the activate command comprises sending an encrypted activate command.

4. The method of claim 3, further comprising the tool decrypting the encrypted activate command.

5. The method of claim 4, wherein decrypting the encrypted activate command is performed using a key stored in the tool.

6. The method of claim 1, further comprising receiving the authorization code of the user from information stored on a smart card.

7. The method of claim 6, wherein receiving the authorization code further comprises receiving a personal identification number code from the user in addition to the information stored on the smart card.

8. The method of claim 6, wherein receiving the information stored on the smart card comprises receiving a digital signature from the smart card.

9. The method of claim 1, further comprising:

providing sensors in the tool; and

communicating data indicating the environment from the sensors to a surface unit.

10. The method of claim 9, wherein the tool contains an explosive, the method further comprising providing additional sensors at a well surface to detect detonation of the explosive.

11. The method of claim 1, further comprising receiving a command to activate the tool from a remote site.

12. The method of claim 11, wherein receiving the command from the remote site comprises receiving the command over a wireless link.

13. The method of claim 12, wherein receiving the command over the wireless link comprises receiving the command over a radio frequency link.

14. A tool, comprising:

a section having an explosive;

a safety sub having a switch;

a first electrical link coupled to the switch and a second electrical link coupled between the switch and the section; and

the switch adapted to isolate the first and second electrical links when the switch is in the open position to disable electrical arming of the section.

15. The tool of claim 14, wherein the section comprises a gun.

16. A system for activating a tool, comprising:

a controller having an interface to communicate with the tool,

the controller further having a security input unit adapted to receive an authorization code,

the controller adapted to verify the authorization code; and

the interface adapted to receive data pertaining to an environment of the tool.

17. The system of claim 16, wherein the controller is adapted to enable activation of the tool in response to verifying the authorization code and data pertaining to the environment of the tool.

18. The system of claim 16, further comprising a communications interface adapted to wirelessly communicate with a remote site.

19. The system of claim 18, wherein the communications interface is adapted to communicate with the remote site using radio frequency signaling.

20. The system of claim 16, wherein the security input unit comprises a smart card reader adapted to receive information stored on a smart card.

21. The system of claim 20, wherein the security input unit is further adapted to receive a password from a user.

22. An assembly comprising:

an activation system having an interface and a security input unit; and

a tool coupled to the interface of the activation system,

the security input unit adapted to receive an authorization code,

the interface adapted to receive data relating to an environment of the tool.

23. The assembly of claim 22, wherein the activation system is adapted to enable activation of the tool based on the authorization code and the environment data.

24. The assembly of claim 23, wherein the activation system is adapted to receive an activate indication from a user, and to send an activate command to the tool in response to activation being enabled.

25. The assembly of claim 24, wherein the tool comprises an explosive device.

26. The assembly of claim 25, wherein the tool comprises a safety sub adapted to electrically isolate a section of the tool containing the explosive device.

27. The assembly of claim 26, wherein the safety sub comprises a switch set to an open position to isolate the section of the tool containing the explosive.

28. The assembly of claim 22, wherein the tool comprises sensors adapted to communicate the environment data to the activation system.

29. The assembly of claim 28, wherein the tool comprises a perforating tool.

30. The assembly of claim 29, further comprising a sensor adapted to be placed at an earth surface to detect firing of the perforating tool.

31. The assembly of claim 22, further comprising a remote system adapted to communicate wirelessly with the activation system.

32. The assembly of claim 31, wherein the remote system is adapted to communicate an activate command to the activation system.

33. The assembly of claim 22, wherein the security input unit comprises a smart card reader.

34. A method of handling a tool containing a section having an explosive device, comprising:

providing a safety sub between the section and an input of the tool; and

setting a switch in the safety sub to an open position to electrically isolate the section from the input.

35. The method of claim 34, further comprising transporting the tool in a prearmed state with the explosive device connected in the section.

36. A method of activating a tool containing an explosive, comprising:

receiving, by a security input device, an authorization code associated with a user;

verifying, based on the authorization code, that the user is authorized to activate the tool containing the explosive; and

sending, in response to user input, one or more messages to the tool containing the explosive to activate the tool.

37. The method of claim 36, wherein receiving the authorization code by the security input device comprises receiving the authorization code from one of a smart card reader and a biometric input device.

38. The method of claim 36, wherein the tool comprises a perforating gun, and wherein sending the one or more messages comprises sending a first message to arm the perforating gun and sending a second message to fire the gun.

39. The method of claim 36, wherein sending the one or more messages comprises sending one or more encrypted messages.

40. The method of claim 39, further comprising the tool decrypting the one or more encrypted messages.

41. The method of claim 36, wherein the tool has plural guns, each gun having a unique code, and wherein sending the one or more messages comprises sending the one or more messages containing the unique codes.

42. The method of claim 41, wherein sending the one or more messages comprises sending one message to all the guns.

43. The method of claim 42, further comprising providing a delay element in each of the guns to specify a delay from receipt of the message to firing of the gun,

wherein the delay in one gun is different form the delay in at least another gun.

44. The method of claim 36, further comprising providing plural access levels, wherein verifying that the user is authorized based on the authorization code comprises determining one of the plural access levels associated with the user.

45. A system comprising:

a security input device adapted to receive an authorization code of a user;

a controller adapted to verify, based on the authorization code, if the user is allowed access to activate a tool containing an explosive device; and

an interface adapted to be coupled to a link to the tool containing the explosive device,

the interface adapted to send an activation message to the tool under control of the controller.

46. The system of claim 45, wherein the security input device comprises one of a smart card reader and a biometric input device.

47. The system of claim 45, further comprising a storage device to store authorization information, the controller adapted to compare the authorization code with the authorization information in the storage device.

48. The system of claim 45, wherein the activation message comprises an encrypted activation message.

49. The system of claim 45, wherein the activation message comprises a message to fire a perforating gun in the tool.

50. An article comprising at least one storage medium containing instructions for controlling a tool having an explosive, the instructions when executed causing a system to:

receive, through a security input device, an authorization code associated with a user;

verify, based on the authorization code, that a user is allowed to activate the tool having the explosive; and

generate one or more messages to send to the tool having the explosive for activating the tool.

51. A tool comprising:

a gun having an explosive and a sensor,

the sensor adapted to communicate data over a communications line coupled to the tool.

52. The tool of claim 51, wherein the gun further comprises at least another sensor adapted to communicate data over the communications line.

53. The tool of claim 51, wherein the sensor is selected from the group consisting of a temperature sensor, pressure sensor, fluid density sensor, moisture detector, strain-gauge bridge sensor, acoustic sensor, vibration sensor, sand detection sensor, water detection sensor, scale detector, viscosity sensor, bubble point sensor, composition sensor, infrared sensor, gamma ray sensor, H_2S sensor, CO_2 sensor, casing collar locator, position sensor, and orientation sensor.

54. The tool of claim 53, wherein the gun has at least another sensor selected from the group.

55. The tool of claim 51, further comprising another gun having an explosive and a sensor.

56. A method for use in a well, comprising:

lowering a tool having a gun into the well;

providing a sensor in the gun; and

communicating data from the sensor over a communications line coupled to the tool.

57. The method of claim 56, further comprising:

providing another gun in the tool; and

providing another sensor in the other gun.

58. The method of claim 56, wherein providing the sensor comprises providing a sensor selected from the group consisting of a temperature sensor, pressure sensor, fluid density sensor, moisture detector, strain- gauge bridge sensor, acoustic sensor, vibration sensor, sand detection sensor, water detection sensor, scale detector, viscosity sensor, bubble point sensor, composition sensor, infrared sensor, gamma ray sensor, H_2S sensor, CO_2 sensor, casing collar locator, position sensor, and orientation sensor.

59. The method of claim 56, further comprising providing another sensor in the gun.

Application No:	GB 0302937.8 30	**Examiner:**	Andrew Hughes
Claims searched:	1-13, 16-33	**Date of search:**	28 May 2003

Patents Act 1977 : Search Report under Section 17

Documents considered to be relevant:

Category	Relevant to claims	Identity of document and passage or figure of particular relevance
		NONE

Categories:

X	Document indicating lack of novelty or inventive step	A	Document indicating technological background and/or state of the art.
Y	Document indicating lack of inventive step if combined with one or more other documents of same category.	P	Document published on or after the declared priority date but before the filing date of this invention.
&	Member of the same patent family	E	Patent document published on or after, but with priority date earlier than, the filing date of this application.

Field of Search:

Search of GB, EP, WO & US patent documents classified in the following areas of the UKC^{V}:

E1F

Worldwide search of patent documents classified in the following areas of the IPC^{7} :

E21B

The following online and other databases have been used in the preparation of this search report :

EPODOC, WPI & JAPIO